Use of CCTV by Kirkwall Grammar School

June 2015

Version 2

KGS should have due regard to this policy to ensure that the use of CCTV follows the Information Commissioner's Office CCTV Code of Practice (2008) and complies with the Data Protection Act 1998 and the Human Rights Act 1998

1. INTRODUCTION

1.1 KGS will use CCTV for a number of reasons - to protect against crime and to protect pupils, staff, parents and members of the public when they are on school premises.

1.2 Images of people captured on CCTV where they can be easily identified are defined as personal data under the Data Protection Act 1998. This means that Orkney Schools must meet the requirements of the Act when using CCTV.

1.3 KGS should have due regard to this policy to ensure that it can justify its use of CCTV under the Data Protection Act 1998 and subsequent guidance released by the Information Commissioner's Office and under the Human Rights Act 1998.

1.4 The policy applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities. Any operation of this kind may only be carried out with reference to the Regulation of Investigatory Powers Act (RIPA) 2000 in consultation with the Council's RIPA office and/or the Police. For further details see section 6.

1.5 This policy applies to all CCTV systems, whether digital (recommended) or analogue.

1.6 This policy will be reviewed as appropriate or as legal advice changes.

2. RESPONSIBILITIES FOR CCTV OPERATION

2.1 CCTV schemes will be administered and managed by the Head teacher in accordance with this policy and with guidance from the Local Authority (LA) where necessary.

2.2 The day-to-day management of the CCTV scheme will be the responsibility of the senior management team during the day and any designated members of staff at evenings, weekends and during school holidays.

2.3 Precautions must be in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to the Data Protection Act 1998 and any security precautions.

2.4 As an annual notification for CCTV use is required, checks or audits need to be carried out on a regular basis to ensure that all procedures are correctly followed, and to justify your use of CCTV.

3. LEGAL BASIS FOR USE OF CCTV SYSTEMS

3.1 The use of CCTV and the images recorded must comply with the Data Protection principles and must be:

- Fairly and lawfully obtained;
- Adequate, relevant and not excessive;
- Accurate;
- Used only for purposes about which people have been informed;
- Secure and protected from unauthorised access;
- Not held longer than required for the purposes they were recorded;
- Accessible to data subjects where a request has been made under the Data Protection Act and where the images are defined as personal data.

3.2 In order to use CCTV, KGS must have a legitimate basis for recording the personal data. The legitimate purposes for which CCTV would be in use in the school are the following:

- Prevention and detection of crime, eg, theft, arson and criminal damage;
- To protect the school buildings and assets;
- To increase the perception of safety and reduce the fear of crime;
- To protect members of the public and private property;
- To ensure the safety of pupils and others present on school premises.

3.3 The use of CCTV must be fair and must not be excessive or prejudicial to any individual or any group of individuals. In order for the use of CCTV to be fair, KGS must inform people that CCTV is in use on their premises by means of notices.

3.4 The Human Rights Act (HRA) gives every individual a right to private life and correspondence. This means that CCTV should not be used inappropriately and in areas where people could expect privacy. The HRA also makes it imperative that people are informed when CCTV is in operation.

3.5 KGS must document the purposes for which CCTV is to be used on the premises.

4. ENSURING THAT USE OF CCTV IS FAIR

4.1 The LA should include the use of CCTV on their annual Data Protection notification (registration) to the Information Commissioner's Office as one of the purposes for which they use personal data.

4.2 KGS must only use CCTV for the purposes they have stated. CCTV or images produced from it should not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

4.3 Prior to installing a system, the school should consult with parents and pupils about the use of CCTV on the school site and with any other nearby residents or business owners who may be affected by its use.

4.4 The school will ensure that pupils, staff and other people who use their buildings are informed of the use and purpose of CCTV. This should be done by means of clear and obvious notices placed around the school premises. Notices should include the following information:

- The identity of the Data Controller (the school);
- The purposes for which CCTV is being used, eg, for the prevention or detection of crime or to increase safety and security whilst on school premises;
- Details of who to contact about the scheme and name/phone number where applicable.

4.5 The precise wording of a notice may vary, but suggested wordings are:

- Warning: these premises are protected by closed circuit television. The images recorded are used for the purposes of crime prevention and public safety
  Operator: Contact:

- For your safety and security and for the prevention of crime, closed circuit television operates in this area.
  Operator: Contact:

4.6 CCTV cameras must only record images on school premises and should not be directed at surrounding private property.

4.7 **The viewing of CCTV footage will be the responsibility of the head teacher and a limited number of nominated staff. Staff or individuals connected to the school or educational setting who wish to view CCTV footage should do so by written request to the responsible person (Appendix ii) and details of the view should be recorded (Appendix i)**

5. SELECTION, OPERATION AND MAINTENANCE OF CCTV SYSTEMS

Selecting a system

5.1 The CCTV system chosen must be of sufficient quality to ensure that recordings and images produced are useable by the school and the Police. When choosing or updating a system, the latest Police guidance (which can be found on the Home Office website) should be used. In general:

- Digital systems are recommended by the Police as they provide good quality recordings and the capacity to produce clips and stills and to copy records to removable media.

- Equipment must work effectively together. For example, a high quality digital CCTV system can only be used to its full capacity if the cameras are also of a similar quality.

- Equipment must be maintained correctly, checked regularly and repaired immediately if faulty, otherwise there is a risk that footage cannot be used in the investigation of a crime.

- Cameras should be sited so that individuals can be recognised easily, where required. Care should be taken that the view from a camera does not become obscured or is positioned to view spaces that is not of relevance to the purposes of your CCTV system.

Security

5.2 CCTV equipment should be held in a separate, locked room where possible (or in a locked cupboard where this is not possible) and access must be strictly confined to authorised staff. Where other staff or visitors need to have access to the system, this should be documented.

5.3 If out of hours emergency maintenance is required the staff member in charge of the CCTV system must be satisfied of the identity of contractors before allowing access to the equipment.

5.4 Remote access to cameras via 'off air' access or via broadband links should be used sparingly. When accessing cameras from home over the Internet, staff should ensure that unauthorised persons cannot view the footage, or safeguards are installed to protect CCTV images from being intercepted.

Retention of recordings

5.5 Digital recordings or removable media (i.e. cassettes/CD's etc) must be stored in a separate, locked room (or locked cupboard) and access must be strictly confined to authorised staff. A recording system i.e. dates/times and recording details should also be retained whilst the material is held.

5.5 Recordings should be held for a limited length of time and must be destroyed when their use is no longer required. A maximum period of 28 days is recommended but this may be extended where the recordings are required for an ongoing investigation. When the retention period has been reached, digital recordings or removable media should be destroyed or wiped securely.

6. COVERT SURVEILLANCE

6.1 On the rare occasions when KGS may wish to use CCTV covertly (ie, without making people aware of it), an application must be made under the Regulation of Investigatory Powers Act (RIPA). The school should discuss the matter with the Single Point of Contact (SPOC) for Orkney Island Council in order to gain authorisation. An application form will need to be filled out and the request will either be accepted or rejected by the SPOC.

6.2 Where the police wish to undertake convert surveillance, they will gain authorisation from their own SPOC.

7. PROCEDURES FOR DISCLOSURE OF CCTV RECORDS TO OTHER ORGANISATIONS

7.1 Access to CCTV recordings day-to-day should be restricted to staff who operate the system.

7.2 CCTV recordings should be held only by the school unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation.

7.3 Records may need to be disclosed for the following reasons:

- To the police, for the prevention and detection of crime;
- To a court for legal proceedings;
- To a solicitor for legal proceedings;
- To the media for the purposes of identification.

7.4 Where recordings have been disclosed or viewed by an authorised third party the school must keep a record of:

- When the images were disclosed;
- Why they have been disclosed;
- Any crime incident number to which they refer;
- Who the images have been viewed by or disclosed to.

7.5 Viewing of CCTV recordings by the Police must be recorded in writing. Requests by the Police are actioned under section 29 of the Data Protection Act. The Police should provide a completed section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the school must record in writing when and why the information has been released.

7.6 Should a recording be required as evidence, a copy may be released to the Police. Where this occurs the recording will remain the property of the school. The date of the release and the purpose for which it is to be used must be recorded.

7.7 The Police may require the school to retain recordings for possible use as evidence in the future. Such records must be stored and indexed so that they can be retrieved when required.

7.8 Applications received from other outside bodies (eg, solicitors) to view or release tapes will be referred to the Head teacher. In these circumstances, tapes may be released where satisfactory evidence is produced showing that they are required for legal proceedings, an information access request (see section 8) or in response to a Court Order.

7.9 Tapes will only be released to the media for use in the investigation of a specific crime and with the written agreement of the Police.

8. SUBJECT ACCESS REQUESTS

8.1 Under section 7 of the Data Protection Act 1998, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act. If a request is received, a fee (up to a maximum £10) can be charged and a copy of the images must be provided within 40 days of the request.

8.2 Recent legal cases have raised the issue of when CCTV images should be considered as personal data. Guidance arising from this implies that personal data must be substantially about the person and should affect their privacy in some way. In relation to CCTV this will not include all images:

- A wide shot of, for example, a playground or school corridor with many people in view of the cameras would not normally be considered as the personal data of all those involved. However, where a camera has picked up an individual or group of individuals specifically, or has been moved to zoom in on them, the images recorded can be considered personal data.

8.3 Where a request has been made to view an image or recording, an application must be made in writing, together with details of themselves to allow you to identify them as the subject of the images and to locate the images on the system. The individual may wish to access either a still image or part of a recording. Where third parties are included in the images, they should be removed where this is technically possible. Where removal is not possible, a balanced decision needs to be made, which considers whether the images would involve an unfair intrusion into the privacy of third parties in the image(s), cause unwarranted harm or distress, and whether it is reasonable in all circumstances to release the information to the individual.

8.4 There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with this policy - see 5.5 (ie, for recordings that no longer exist). However, where a request has been made for recordings still in existence, they must not be destroyed until the request is complete.

8.4 For further information on dealing with requests under the Data Protection Act, the Orkney Islands Council's (OIC) publication Personal Information Your right to know, which is available on the OIC website: http://www.orkney.gov.uk/Council/D/Data-Protection-Policy.htm. Where queries arise, please contact the OIC's Information Governance Officer.

9. BREACHES OF POLICY

9.1 Any breach or alleged breach of this policy or school guidelines on the use of CCTV by school staff or other individuals should be investigated by the Head teacher.

9.2 An investigation should be carried out into any breaches of policy and procedures reviewed or put in place to ensure that the situation does not arise again.

10. COMPLAINTS

10.1 Any complaints about the operation of the CCTV system should be addressed to the Head teacher, where they will be dealt with according to the school's standard complaints procedures, with reference to this policy.

REFERENCES AND LINKS

Information Commissioners Office: ico.org.uk

Orkney Islands Council Data Protection webpage:
http://www.orkney.gov.uk/Council/D/Data-Protection-Policy.htm

CCTV Code of Practice (revised edition 2008): Code of Practice